PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04N 7/167, 7/16, 5/00

A1

(11) International Publication Number: WO 98/56179

(43) International Publication Date: 10 December 1998 (10.12.98)

(21) International Application Number: PCT/US98/11633

(22) International Filing Date: 5 June 1998 (05.06.98)

(30) Priority Data:
60/048,819 6 June 1997 (06.06.97) US

(71) Applicant *(for all designated States except US)*: THOMSON CONSUMER ELECTRONICS, INC. [US/US]; 10330 North Meridian Street, Indianapolis, IN 46290–1024 (US).

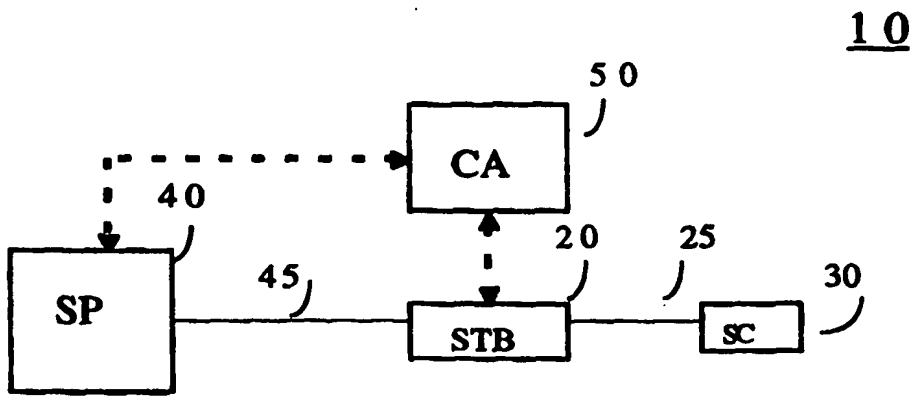
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ESKICIOGLU, Ahmet, Mursit [TR/US]; 8235 Lakeshore Trail No. 125, Indianapolis, IN 46250 (US). WEHMEYER, Keith, Reynolds [US/US]; 6411 Columbia Circle, Fishers, IN 46038 (US). VIRAG, David, Emery [US/US]; 7485 Cherry Hill Drive, Indianapolis, IN 46254 (US).

(74) Agents: TRIPOLI, Joseph, S. et al.; GE & RCA Licensing Management Operation, Inc., P.O. Box 5312, Princeton, NJ 08543 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: CONDITIONAL ACCESS SYSTEM FOR SET–TOP BOXES



(57) Abstract

A system conditionally establishes a communication channel between two devices only if one device is authenticated by the other device. Authentication of the second device by the first device involves sending a message to the second device; receiving, from the second device, the message encrypted using a private key of the second device and a digital certificate having a public key of the second device; decrypting the digital certificate to obtain the public key, using the public key to decrypt the message and comparing the decrypted message to the message originally sent to the second device.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

CONDITIONAL ACCESS SYSTEM FOR SET-TOP BOXES

Field of the Invention

This invention concerns a system for providing conditional access (i.e., managing access) to a device, such as a "consumer electronic device". Examples of such consumer electronic devices include separate devices or "boxes" that may be located on top of, and coupled to a television receiver, i.e., set-top boxes.

Background of the Invention

In general, conditional access involves limiting or controlling the communication with a device based on predetermined criteria. Conditional access may be achieved by connecting two devices together when communication therebetween is desired and by disconnecting the two devices from one another when such communication is no longer desired. However, in the context of today's sophisticated computer networks interconnected to form what is known as the world-wide web ("web"), many, if not all, of the devices designed to communicate with the web are "permanently" connected to the web through modem hookups or other means. That is, the devices usually remain physically connected to the web. Typically, access to the web is via a specially designed software package loaded onto a computer and a modem; this software enables a user to connect to an internet service provider who acts as the gate keeper to the web. The user typically pays a monthly fee to the service provider for access to the internet, either on a limited or unlimited basis. The proliferation of users who regularly access the

web as a source of information or even as a means of communicating via E-Mail for both business and personal reasons has created a very competitive market for both service providers and the manufacturers of the necessary hardware. Thus, as one would expect there are numerous service providers, each requiring specialized software for access.

An outgrowth of today's emerging digital consumer electronic products is an opportunity to access the Internet from a user's television. Such access has been accomplished by utilizing the user's television as a monitor or display device in conjunction with a set-top box that provides the software (e.g., a web browser) and hardware (e.g., modem, ethernet, ADSL or any equivalent connection means) needed to interface to the web. For example, the RCA Network Computer manufactured by Thomson Consumer Electronics is such a set-top box that may be connected to both a television and a phone line or the like thereby permitting the user to access the web. Set-top boxes may provide a means for a variety of internet applications (e.g., electronic commerce) from the home, the office or any location without utilizing a personal computer or any general purpose computing device. These set-top boxes have open hardware architectures which would permit easy adaptation of the set-top box thereby permitting use with any of a plurality of service providers.

Summary of the Invention

The manufacturers of these set-top boxes may desire that the box only be used with selected service providers. For example, the manufacturer of the box may be compensated by the service provider

for each connection to the service from the box. Thus, the flexibility of the set-top box's open hardware architecture in combination with a competitive market for such devices necessitates the need to provide a system for providing conditional access in the set-top box so that the box can only connect to selected service providers. This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem.

Generally, the present invention defines a method for managing access to a device by sending a first message to a second device; receiving a digital certificate encrypted using a first private key; receiving the first message encrypted using a second private key; authenticating the second device; and establishing a communication channel between the devices.

In accordance with one aspect of the present invention, the first message comprises data associated with the first device and a date and time stamp, and the digital certificate comprises data associated with the second device and a second public key.

In accordance with another aspect of the present invention, the step of authenticating comprises decrypting the digital certificate using a first public key; decrypting the first encrypted message using the second public key to generate a first decrypted message; and comparing the first decrypted message to the first message.

In accordance with another aspect of the present invention, the method further comprises providing confirmation of

the authentication to said second device by encrypting the first message using the second public key to generate a second encrypted message; and sending the second encrypted message to the second device.

In accordance with still another aspect of the present invention, the digital certificate, the first public and first private keys are issued by an independent certificate authority and are associated with the second device.

In accordance with yet another aspect of the present invention, a system for managing access between a service provider and a set-top box having a smart card coupled thereto, the set-top box sends a first message to the smart card; receives a smart card (first) digital certificate encrypted using a private key; authenticates the smart card; contacts the service provider and sends a second message to the service provider; receives a service provider (second) digital certificate encrypted using another private key; receives the second message encrypted using yet another private key; authenticates the service provider; provides confirmation to the service provider; and establishes a communication channel with the service provider. Particularly, the two messages contain at least set-top box identification data.

In accordance with yet another aspect of the present invention, the smart card includes service provider identification data associated with a plurality of service providers.

These and other aspects of the invention will be explained with reference to a preferred embodiment of the invention shown in the accompanying Drawings.

Brief Description of the Drawings

Figure 1 is a block diagram of an exemplary implementation of a system for managing access to a device in accordance with the invention; and

Figure 2 is a flowchart diagram of an exemplary implementation of the conditional access system of Figure 1.

Figure 3 is a block diagram of an exemplary implementation of the system of Figure 1 wherein any one of a plurality of set-top boxes may communicate with any one of a plurality of service providers.

Detailed Description of the Drawings

The present invention provides a conditional access system which may be utilized to obtain services from one of a plurality of sources. When implemented within a set-top box, the conditional access system permits the set-top box to authenticate the service provider and/or a smart card used to access services before a communication channel is established. Such a conditional access system may act as a toll bridge for access to services, thereby permitting a mechanism for the manufacturer of the set-top box to collect fees based on use of its set-top box.

In Figure 1, the system 10 for managing access to a set-top box (STB) 20, for example, the RCA Network Computer, is depicted. Smart Card (SC) 30 is inserted into or coupled to a smart card reader (not shown) included in STB 20; an internal bus 25 interconnects STB 20 and SC 30 thereby permitting the transfer of data therebetween. Alternately, the functionality of the smart card may be embedded within the set-top box. STB 20 is connected to service provider (SP) 40 via a dial-up link or a direct link, which is depicted as element 45. Certificate Authority (CA) 50 is not directly connected to either SP 40 or STB 20 but issues digital certificates and public and private key pairs, which are used as explained below. These digital certificates are used by service providers and smart card manufacturers. It is within the scope of this invention that the digital certificates could be provided via an on-line connection. Further, it is within the scope of this invention that the role of Certificate Authority may be performed by SP 40 in collaboration with the manufacturer of the STB 20. The conditional access system of the present invention will be described in relation to system 10 as shown in Figure 1 and the flowchart diagram of Figure 2.

This conditional access system is based on authentication of each device (for example, SC 30 and SP 40) communicating with STB 20 prior to establishing a communication channel between a STB 20 and SP 40. Particularly, this conditional access system utilizes an asymmetric key system (i.e., public-key system), wherein only public keys are stored in the set-top box. That is, the set-top box does not store or contain any secrets (i.e., private keys). The foundation of public-key cryptography is the use of two related keys, one public

and one private; the private key being computationally unfeasible of being deduced from the public key which is publicly available. Anyone with a public key can encrypt a message but only the person or device having the associated and predetermined private key can decrypt it. Similarly, a message can be encrypted by a private key and anyone with access to the public key can decrypt that message. Encrypting messages using a private key may be referred to as "signing" because anyone holding the public key can verify that the message was sent by the party having the private key. This may be thought of as being analogous to verifying a signature on a document.

A digital certificate or certificate is a message sent in the clear (i.e., unencrypted) having a CA 50 signature attached thereto; thus the recipient of the certificate can verify the source or origin of the certificate. These digital certificates are in fact "signed messages" because the signature attached to the message is produced by encrypting either the message itself or a digest of the message (which is obtained by hashing the message, as described later). Unilateral authentication of each device connected to the set-top box is achieved by passing such certificates between the devices and verifying these certificates. Certificate verification involves checking the signature by decryption. These certificates may contain information used by the device receiving the certificate. This information may be related to a device not involved in the passing of this certificate, e.g. information contained in the first digital certificate is related to the service provider as described below. Further, the certificates may contain information associated with the device passing the certificate and a public key of the passing device.

As described above, only public keys are stored in a memory device contained in STB 20. Further, the first and second digital certificates, which may be issued by CA 50, are stored in SC 30 and SP 40, respectively.

The following nomenclature will be utilized in the below description of the present conditional access system.

KCApri1	Private key used to create SC's certificate
KCApub1	Public key used to verify SC's certificate
KCApri2	Private key used to create SP's certificate
KCApub2	Public key used to verify SP's certificate
KSPpub	SP's Public key
KSPpri	SP's Private key

These are used and discussed with respect to authenticating a device such as the smart card or the service provider.

After STB 20 is activated and SC 30 is inserted into STB 20, STB 20 sends a first message to SC 30 (see Figure 2, Step 100). This first message contains identification data corresponding to STB 20, for example, such identification data may include the manufacturer's identification data (MID). In response to the first message, SC 30 replies by sending a first digital certificate back to STB 20 (see Figure 2, Step 120). The first digital certificate (i.e., SC's certificate) includes data sent in the clear and an attached signature which is encrypted using KCApri1, the private key which is used to create certificates sent by SC 30. This data may include identification

data corresponding to a selected service provider having a pre-existing agreement with the manufacturer of STB 20. Particularly, this data may also include, in addition to the service provider identification data, a phone number for the service provider which will be used for contacting the service provider as described below.

If SC 30 does not have a digital certificate associated with a service provider (see Figure 2, Step 110), STB 20 may contact an independent party (not shown), download an appropriate digital certificates from the independent party (see Figure 2, Step 114) and transfer them to SC 30 (see Figure 2, Step 116). STB 20 may contact the independent party utilizing an integrated modem. If the digital certificates are downloaded from the independent party, the above process may continue starting at the point where SC 30 replies to the first message by sending a first digital certificate back to STB 20.

Now, STB 20 must authenticate (see Figure 2, Step 130) SC 30 by verifying that SC 30 has passed a valid certificate to STB 20, this involves decrypting the first digital certificate in STB 20 using KCApub1. KCApub1, which is stored in STB 20, is the corresponding public key also assigned by CA 50. After SC 30 is authenticated, the service provider identification data included in the first digital certificate is used by STB 20 to contact the desired service provider, for example SP 40.

SC 30 may have more than one digital certificate, each one of which may identify a different service provider. If this is the case, the user may be prompted to select one of the service providers having a valid certificate (see Figure 2, Step 140). Further, if a

service provider has more than one access number, the set-top box may select an alternate number if, for example, the primary number is busy.

STB 20 sends a second message to SP 40 (see Figure 2, Step 150); this second message contains similar identification data corresponding to STB 20. For example, such identification data now may include the manufacturer's identification data (MID) and a date and time stamp (DTS). DTS may be downloaded from an electronic program guide or from a special time server or possible through an internal means. In response to the second message, SP 40 replies by sending (1) a second digital certificate (i.e., SP's certificate) and (2) the second message encrypted using KSPpri back to STB 20 (see Figure 2, Step 160). The second digital certificate includes data sent in the clear and an attached signature which is created using KCApri2. This data may include identification data corresponding to the service provider, the validity period (VP) for the second digital certificate and the public key for SP 40, i.e., KSPpub. The identification data may also further include data associated with CA 50 which may be utilized, if necessary, for authentication of SP 40. Now SP 40 must be authenticated; such authentication is achieved utilizing the second digital certificate and the encrypted second message (see Figure 2, Step 170).

Particularly, authentication of the service provider involves (1) decrypting the second digital certificate in STB 20 using KCApub2, which is stored therein, (2) decrypting the encrypted second message using the public key of SP 40 (i.e., KSPpub) which is included in the second digital certificate and (3) comparing the

decrypted "encrypted second message" to the original second message sent to SP 40. This ensures that the certificate was received from the desired service provider and not from another source.

Further, the data contained in the second digital certificate may be subjected to a one-way hashing algorithm, such as MD5 developed by Ron Rivest or SHA-1 developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) prior to being encrypted by KCApri2. If this is the case, authentication may also include hashing the data sent in the clear using the same one-way hashing algorithm and comparing this data to the decrypted data. Similarly, the creation of the first digital certificate may involve the use of such a one-way hashing algorithm.

After SP 40 has been authenticated by STB 20, STB 20 sends confirmation of this authentication back to SP 40 (see Figure 2, Step 180). This confirmation involves sending the second message now being encrypted using the public key of SP 40, i.e., KSPpub, back to SP 40. SP 40 can decrypt this message using its associated private key, KSPpri. Finally, STB 20 establishes a communication channel (see Figure 2, Step 190) between STB 20 and SP 40 wherein all future communication may be handled utilizing public-key cryptography and the public and private key pairs associated with SP 40 (i.e. KSPpub and KSPpri).

The present invention has been described in terms of an exemplary embodiment in which a single smart card cooperates with a single set-top box to manage access to a single service provider. However, it is within the scope of this invention to provide a

conditional access system which may be extended to permit the smart card to "roam" across (i.e., provide conditional access between) multiple service providers and multiple manufacturers of the set-top boxes. This is particularly illustrated in Figure 3 where SC 30a may be used in any one of STBs 20a, 20b or 20c to access any one of SPs 40a, 40b or 40c. In such a system, each set-top box manufacturer will have a unique MID. The smart card will have a unique first digital certificate for each service provider and for each manufacturer having a predetermined agreement with the service provider. Each set-top box will have unique sets of public keys for verifying these digital certificates. For example, if there are "m" service providers and "n" manufacturers of set-top boxes then the smart card may contain up to "m times n" number of digital certificates.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon a reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in the art and it is intended to include such alterations within the scope of the appended claims. Further, it is within the scope of the present invention that the conditional access system defined herein is fully capable of being utilized between any two devices interconnected.

Claims

1. A method for managing access to a device, said method comprising:

(a) sending a first message from a first device to a second device;

(b) receiving from said second device a digital certificate encrypted using a first private key of said second device;

(c) receiving from said second device said first message encrypted using a second private key of said second device;

(d) authenticating said second device in response to said digital certificate and said first encrypted message; and

(e) establishing a communication channel between said first and said second devices in response to the authentication of said second device.

2. The method of Claim 1 wherein said first message comprises first identification data associated with said first device and a date and time stamp.

3. The method of Claim 2 wherein said digital certificate comprises second identification data associated with said second device and a second public key of said second device.

4. The method of Claim 3 wherein the step of authenticating comprises the steps of:

(a) decrypting said digital certificate in said first device using a first public key;

(b) decrypting said first encrypted message using said second public key to generate a first decrypted message; and

(c) comparing said first decrypted message to said first message.

5. The method of Claim 4 wherein said first public key is stored in said first device.

6. The method of Claim 5 further comprising the step of providing confirmation of the authentication to said second device by

(a) encrypting said first message using said second public key to generate a second encrypted message; and

(b) sending said second encrypted message to said second device.

7. The method of Claim 6 wherein said digital certificate, said first public key and said first private key are issued by an independent certificate authority and are associated with said second device.

8. The method of Claim 1 wherein said first device is a set-top box and said second device is a server associated with a service provider.

9. The method of Claim 8 wherein said second identification data further comprises data associated with said certificate authority and data associated with the validity of said digital certificate.

10. A method for managing access to a device, said method comprising:

(a) sending first identification data associated with a first device to a second device;

(b) receiving from said second device a digital certificate encrypted using a first private key of said second device, said digital certificate having second identification data associated with said second device and a second public key of said second device; (c) encrypting said first identification data in said second device using a second private key associated with said second device to generate first encrypted identification data;

(d) receiving from said second device said first encrypted identification data;

(e) decrypting in said first device, using a first public key to obtain said second public key, said encrypted digital certificate received from said second device, said first public key being stored in said first device;

(f) decrypting said first encrypted identification data using said second public key to generate a first decrypted identification data;

(g) authenticating said second device by comparing said first decrypted identification data to said first identification data;

(h) sending to said second device second encrypted identification data, said second encrypted identification data being encrypted in said first device using said second public key of said second device; and

(i) establishing a communication channel between said first and said second devices.

11. In combination in a system for managing access between a service provider and a set-top box having a smart card coupled thereto, said set-top box performing the steps of:

(a) sending a first message to the smart card, said first message containing set-top box identification data;

(b) receiving from the smart card, in response to said first message, a first digital certificate encrypted using a first private key, said first digital certificate containing service provider identification data;

(c) authenticating the smart card in response to said first digital certificate;

(d) contacting the service provider in response to the authentication of the smart card and said service provider identification data and sending a second message to the service provider, said second message containing set-top box identification data;

(e) receiving from the service provider, in response to said second message, a second digital certificate encrypted using a second private key of said service provider;

(f) receiving from the service provider said second message encrypted using a third private key;

(g) authenticating the service provider in response to said second digital certificate and said second encrypted message;

(h) providing confirmation of the authentication to the service provider; and

(i) establishing a communication channel with the service provider in response to the authenticated service provider.

12. The combination of Claim 11 wherein the smart card comprises a plurality of digital certificates, each one containing service provider identification data associated with a unique service provider.

13. The combination of Claim 12 wherein the step of authenticating the smart card in response to said first digital certificate comprises decrypting said first digital certificate in said set-top box using a first public key.

14. The combination of Claim 13 wherein said second digital certificate comprises second service provider identification data and a second public key of said service provider.

15. The combination of Claim 14 wherein the step of authenticating the service provider comprises the steps of:

(a) decrypting said second digital certificate in the set-top box using said second public key;

(b) decrypting said encrypted second message using a third public key to generate a second decrypted message; and

(c) comparing said second decrypted message to said second message.

16. The combination of Claim 15 wherein said first public key, said second public key, said first message and said second message are stored in said set-top box.

17. The combination of Claim 16 wherein said first digital certificate, said first private key and said first public key are issued by an independent certificate authority.

18. The combination of Claim 17 wherein said first digital certificate is stored in said smart card.

19. The combination of Claim 18 wherein said second digital certificate, said second private key and said second public key are issued by an independent certificate authority and are associated with said service provider.

5

20. The combination of Claim 19 wherein said second digital certificate is stored in said service provider.

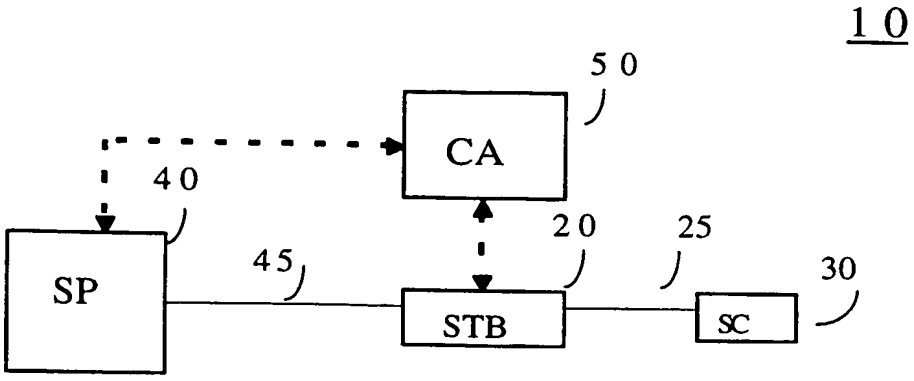


Fig 1.

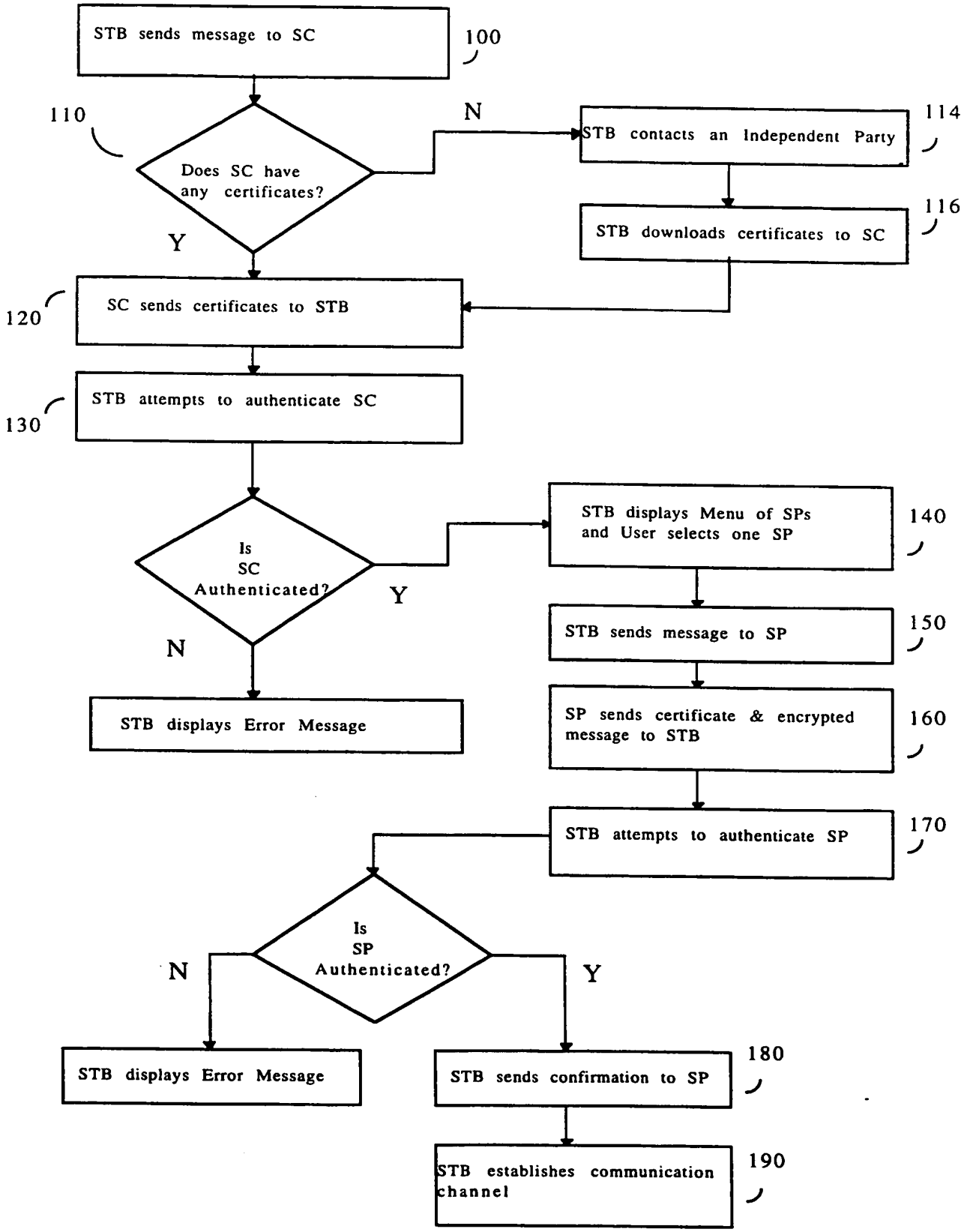

STB sends message to SC
100
110
Does SC have any certificates?
N
Y
STB contacts an Independent Party
114
STB downloads certificates to SC
116
120
SC sends certificates to STB
130
STB attempts to authenticate SC
Is SC Authenticated?
Y
N
STB displays Menu of SPs and User selects one SP
140
STB sends message to SP
150
SP sends certificate & encrypted message to STB
160
STB attempts to authenticate SP
170
Is SP Authenticated?
N
Y
STB displays Error Message
STB sends confirmation to SP
180
STB establishes communication channel
190

Fig 2.

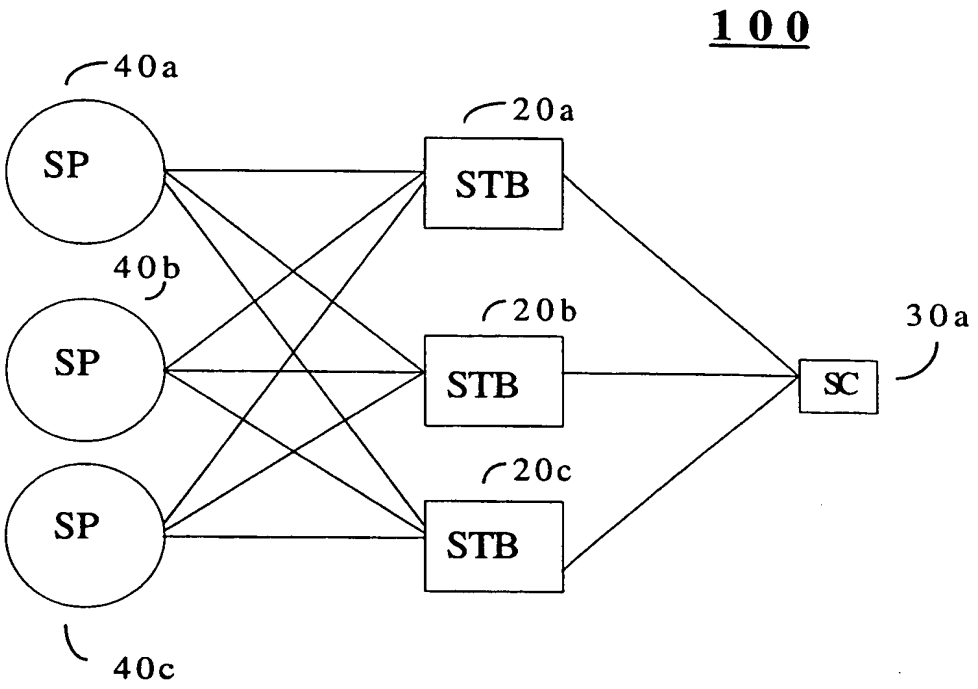


Fig. 3

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
RCA 88637		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US 98/ 11633	05/06/1998	06/06/1997
Applicant		
THOMSON CONSUMER ELECTRONICS, INC. et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. [ ] **Certain claims were found unsearchable** (see Box I).

2. [ ] **Unity of invention is lacking** (see Box II).

3. [ ] The international application contains disclosure of a **nucleotide and/or amino acid sequence listing** and the international search was carried out on the basis of the sequence listing
   - [ ] filed with the international application.
   - [ ] furnished by the applicant separately from the international application,
     - [ ] but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.
   - [ ] Transcribed by this Authority

4. With regard to the **title,**
   - [X] the text is approved as submitted by the applicant
   - [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   - [X] the text is approved as submitted by the applicant
   - [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this International Search Report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is:
   Figure No. 1
   - [X] as suggested by the applicant.
   - [ ] because the applicant failed to suggest a figure.
   - [ ] because this figure better characterizes the invention.
   - [ ] None of the figures.

INTERNATIONAL SEARCH REPORT

In tional Application No
PCT/US 98/11633

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/167 H04N7/16 H04N5/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 438 154 A (CANON KK) 24 July 1991 see column 7, line 16 - column 13, line 7 see figures 1A,1B,3 ---	1-20
A	EP 0 719 045 A (MITSUBISHI CORP) 26 June 1996 see the whole document ---	1-20
A	OMURA J K: "NOVEL APPLICATIONS OF CRYPTOGRAPHY IN DIGITAL COMMUNICATIONS" IEEE COMMUNICATIONS MAGAZINE, vol. 28, no. 5, 1 May 1990, pages 21-29, XP000132493 see page 21, left-hand column, line 13 - page 24, right-hand column, line 25 see figures 1A-D,2,3 --- -/--	1-20

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 September 1998	11/09/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hampson, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/11633

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 97 38530 A (DIGCO B V ;RIX SIMON PAUL ASHLEY (ZA); GLASSPOOL ANDREW (GB); DAVI) 16 October 1997 see abstract see page 4, line 6 - page 5, line 17 see figure 2	1-20
P,A	EP 0 817 485 A (THOMSON MULTIMEDIA SA) 7 January 1998 see abstract see column 5, line 39 - column 8, line 11 see figures 4A,4B,5	1-20

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/11633

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0438154 A	24-07-1991	JP 3214834 A	20-09-1991
		DE 69126801 D	21-08-1997
		DE 69126801 T	05-02-1998
		US 5159633 A	27-10-1992
EP 0719045 A	26-06-1996	JP 8288940 A	01-11-1996
		US 5740246 A	14-04-1998
WO 9738530 A	16-10-1997	AU 2506397 A	29-10-1997
		HR 970160 A	28-02-1998
EP 0817485 A	07-01-1998	FR 2750554 A	02-01-1998
		CN 1171015 A	21-01-1998
		JP 10164052 A	19-06-1998

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 03 February 1999 (03.02.99)	
International application No. PCT/US98/11633	**Applicant's or agent's file reference** RCA 88637
International filing date (day/month/year) 05 June 1998 (05.06.98)	**Priority date** (day/month/year) 06 June 1997 (06.06.97)
Applicant ESKICIOGLU, Ahmet, Mursit et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

21 December 1998 (21.12.98)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer S. Baharlou
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Form PCT/IB/331 (July 1992) 2457310

19

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
RCA 88637		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US98/11633	05/06/1998	06/06/1997
International Patent Classification (IPC) or national classification and IPC H04N7/167		
Applicant THOMSON CONSUMER ELECTRONICS, INC. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
21/12/1998	26.05.99
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Authorized officer Glendinning, D Telephone No. (+49-89) 2399 2443

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US98/11633

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-12	as originally filed				

Claims, No.:

1-20	as received on	10/05/1999	with letter of	06/05/1999	

Drawings, sheets:

1/3-3/3	as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-20
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-20
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

V Reasoned statement under Article 35(2)

Public key encryption systems are known in the prior art, but the documents cited in the Search Report do not disclose or suggest, either individually or taken in any combination, a method whereby

a) a first device sends a first message to a second device
b) the first device receives from the second device a digital certificate encrypted using a first private key of the second device
c) the first device receives from the second device the first message encrypted using a second private key of the second device
d) the second device is authenticated in response to the digital certificate and first encrypted message
e) communication is established between the two devices where the authentication is positive,

so that the subject matter of claim 1 can be said to be new and to have inventive step. The features of claim 1 are included within independent claims 10 and 11, so the same conclusion holds for those claims, as it does for all dependent claims.

VIII Certain observations on the international application

1 Claim 11 is obscure in that although it is directed to a system for managing access between a service provider and a set-top box what it actually defines are method steps performed by the set-top box itself. It would appear that claim 11 should be directed to "A method for managing access between a service provider and a set-top box having a smart card coupled thereto, whereby the set-top box performs the steps of:".

2 Dependent claims 12-20 should then be directed to "The method of claim....".

Claims

1. A method for managing access to a device, said method comprising:

(a) sending a first message from a first device to a second device;

(b) receiving from said second device a digital certificate encrypted using a first private key of said second device;

(c) receiving from said second device said first message encrypted using a second private key of said second device;

(d) authenticating said second device in response to said digital certificate and said first encrypted message; and

(e) establishing a communication channel between said first and said second devices in response to the authentication of said second device.

2. The method of Claim 1 wherein said first message comprises first identification data associated with said first device and a date and time stamp.

3. The method of Claim 2 wherein said digital certificate comprises second identification data associated with said second device and a second public key of said second device.

4. The method of Claim 3 wherein the step of authenticating comprises the steps of:

(a) decrypting said digital certificate in said first device using a first public key;

(b) decrypting said first encrypted message using said second public key to generate a first decrypted message; and

Replaced by Att. 34

(c) comparing said first decrypted message to said first message.

5. The method of Claim 4 wherein said first public key is stored in said first device.

6. The method of Claim 5 further comprising the step of providing confirmation of the authentication to said second device by

(a) encrypting said first message using said second public key to generate a second encrypted message; and

(b) sending said second encrypted message to said second device.

7. The method of Claim 6 wherein said digital certificate, said first public key and said first private key are issued by an independent certificate authority and are associated with said second device.

8. The method of Claim 1 wherein said first device is a set-top box and said second device is a server associated with a service provider.

9. The method of Claim 8 wherein said second identification data further comprises data associated with said certificate authority and data associated with the validity of said digital certificate.

10. A method for managing access to a device, said method comprising:

(a) sending first identification data associated with a first device to a second device;

(b) receiving from said second device a digital certificate encrypted using a first private key of said second device, said digital certificate having second identification data associated with said second device and a second public key of said second device; (c) encrypting said first identification data in said second device using a second private key associated with said second device to generate first encrypted identification data;

(d) receiving from said second device said first encrypted identification data;

(e) decrypting in said first device, using a first public key to obtain said second public key, said encrypted digital certificate received from said second device, said first public key being stored in said first device;

(f) decrypting said first encrypted identification data using said second public key to generate a first decrypted identification data;

(g) authenticating said second device by comparing said first decrypted identification data to said first identification data;

(h) sending to said second device second encrypted identification data, said second encrypted identification data being encrypted in said first device using said second public key of said second device; and

(i) establishing a communication channel between said first and said second devices.

11. In combination in a system for managing access between a service provider and a set-top box having a smart card coupled thereto, said set-top box performing the steps of:

(a) sending a first message to the smart card, said first message containing set-top box identification data;

(b) receiving from the smart card, in response to said first message, a first digital certificate encrypted using a first private key, said first digital certificate containing service provider identification data;

(c) authenticating the smart card in response to said first digital certificate;

(d) contacting the service provider in response to the authentication of the smart card and said service provider identification data and sending a second message to the service provider, said second message containing set-top box identification data;

(e) receiving from the service provider, in response to said second message, a second digital certificate encrypted using a second private key of said service provider;

(f) receiving from the service provider said second message encrypted using a third private key;

(g) authenticating the service provider in response to said second digital certificate and said second encrypted message;

(h) providing confirmation of the authentication to the service provider; and

(i) establishing a communication channel with the service provider in response to the authenticated service provider.

12. The combination of Claim 11 wherein the smart card comprises a plurality of digital certificates, each one containing service provider identification data associated with a unique service provider.

13. The combination of Claim 12 wherein the step of authenticating the smart card in response to said first digital certificate comprises decrypting said first digital certificate in said set-top box using a first public key.

14. The combination of Claim 13 wherein said second digital certificate comprises second service provider identification data and a second public key of said service provider.

15. The combination of Claim 14 wherein the step of authenticating the service provider comprises the steps of:

(a) decrypting said second digital certificate in the set-top box using said second public key;

(b) decrypting said encrypted second message using a third public key to generate a second decrypted message; and

(c) comparing said second decrypted message to said second message.

16. The combination of Claim 15 wherein said first public key, said second public key, said first message and said second message are stored in said set-top box.

17. The combination of Claim 16 wherein said first digital certificate, said first private key and said first public key are issued by an independent certificate authority.

18. The combination of Claim 17 wherein said first digital certificate is stored in said smart card.

19. The combination of Claim 18 wherein said second digital certificate, said second private key and said second public key are issued by an independent certificate authority and are associated with said service provider.

5

20. The combination of Claim 19 wherein said second digital certificate is stored in said service provider.

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

TRIPOLI, Joseph, S.
GE & RCA Licensing Management Opera
P.O. Box 5312
Princeton, NJ 08543
ETATS-UNIS D'AMERIQUE

JUN 03 1999

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Rule 71.1)

Date of mailing *(day/month/year)*	26.05.99
Applicant's or agent's file reference: RCA 88637	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US98/11633	05/06/1998	06/06/1997

Applicant
THOMSON CONSUMER ELECTRONICS, INC. et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Eriksson, I Tel.(+49-89) 2399-2432

Form PCT/IPEA/416 (July 1992)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
RCA 88637		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US98/11633	05/06/1998	06/06/1997
International Patent Classification (IPC) or national classification and IPC H04N7/167		
Applicant THOMSON CONSUMER ELECTRONICS, INC. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
21/12/1998	26.05.99
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Authorized officer Glendinning, D Telephone No. (+49-89) 2399 2443

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US98/11633

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-12	as originally filed			

Claims, No.:

1-20	as received on	10/05/1999	with letter of	06/05/1999

Drawings, sheets:

1/3-3/3	as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-20
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-20
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

V Reasoned statement under Article 35(2)

Public key encryption systems are known in the prior art, but the documents cited in the Search Report do not disclose or suggest, either individually or taken in any combination, a method whereby

a) a first device sends a first message to a second device
b) the first device receives from the second device a digital certificate encrypted using a first private key of the second device
c) the first device receives from the second device the first message encrypted using a second private key of the second device
d) the second device is authenticated in response to the digital certificate and first encrypted message
e) communication is established between the two devices where the authentication is positive,

so that the subject matter of claim 1 can be said to be new and to have inventive step. The features of claim 1 are included within independent claims 10 and 11, so the same conclusion holds for those claims, as it does for all dependent claims.

VIII Certain observations on the international application

1 Claim 11 is obscure in that although it is directed to a system for managing access between a service provider and a set-top box what it actually defines are method steps performed by the set-top box itself. It would appear that claim 11 should be directed to "A method for managing access between a service provider and a set-top box having a smart card coupled thereto, whereby the set-top box performs the steps of:".

2 Dependent claims 12-20 should then be directed to "The method of claim....".

1. A method for managing access to a device, said method comprising:

(a) sending a first message from a first device to a second device;

(b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device;

(c) receiving, in said first device, from said second device said first message encrypted using a second private key of said second device;

(d) authenticating said second device in response to said digital certificate and said first encrypted message; and

(e) establishing a communication channel between said first and said second devices in response to the authentication of said second device.

2. The method of Claim 1 wherein said first message comprises first identification data associated with said first device and a date and time stamp.

3. The method of Claim 2 wherein said digital certificate comprises second identification data associated with said second device and a second public key of said second device.

4. The method of Claim 3 wherein the step of authenticating comprises the steps of:

(a) decrypting said digital certificate in said first device using a first public key;

(b) decrypting said first encrypted message using said second public key to generate a first decrypted message; and

(c) comparing said first decrypted message to said first message.

5. The method of Claim 4 wherein said first public key is stored in said first device.

6. The method of Claim 5 further comprising the step of providing confirmation of the authentication to said second device by

(a) encrypting said first message using said second public key to generate a second encrypted message; and

(b) sending said second encrypted message to said second device.

7. The method of Claim 6 wherein said digital certificate, said first public key and said first private key are issued by an independent certificate authority and are associated with said second device.

8. The method of Claim 1 wherein said first device is a set-top box and said second device is a server associated with a service provider.

9. The method of Claim 8 wherein said second identification data further comprises data associated with said certificate authority and data associated with the validity of said digital certificate.

10. A method for managing access to a device, said method comprising:

(a) sending first identification data associated with a first device to a second device;

(b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device, said digital certificate having second identification data associated with said second device and a second public key of said second device;

(c) encrypting said first identification data in said second device using a second private key associated with said second device to generate first encrypted identification data;

(d) receiving, in said first device, from said second device said first encrypted identification data;

(e) decrypting in said first device, using a first public key to obtain said second public key, said encrypted digital certificate received from said second device, said first public key being stored in said first device;

(f) decrypting said first encrypted identification data using said second public key to generate a first decrypted identification data;

(g) authenticating said second device by comparing said first decrypted identification data to said first identification data;

(h) sending to said second device second encrypted identification data, said second encrypted identification data being encrypted in said first device using said second public key of said second device; and

(i) establishing a communication channel between said first and said second devices.

11. A system for managing access between a service provider and a set-top box having a smart card coupled thereto, said set-top box performing the steps of:

(a) sending a first message to the smart card, said first message containing set-top box identification data;

(b) receiving from the smart card, in response to said first message, a first digital certificate encrypted using a first private key, said first digital certificate containing service provider identification data;

(c) authenticating the smart card in response to said first digital certificate;

(d) contacting the service provider in response to the authentication of the smart card and said service provider identification data and sending a second message to the service provider, said second message containing set-top box identification data;

(e) receiving from the service provider, in response to said second message, a second digital certificate encrypted using a second private key of said service provider;

(f) receiving from the service provider said second message encrypted using a third private key;

(g) authenticating the service provider in response to said second digital certificate and said second encrypted message;

(h) providing confirmation of the authentication to the service provider; and

(i) establishing a communication channel with the service provider in response to the authenticated service provider.

12. The system of Claim 11 wherein the smart card comprises a plurality of digital certificates, each one containing service provider identification data associated with a unique service provider.

13. The system of Claim 12 wherein the step of authenticating the smart card in response to said first digital certificate comprises decrypting said first digital certificate in said set-top box using a first public key.

14. The system of Claim 13 wherein said second digital certificate comprises second service provider identification data and a second public key of said service provider.

15. The system of Claim 14 wherein the step of authenticating the service provider comprises the steps of:

(a) decrypting said second digital certificate in the set-top box using said second public key;

(b) decrypting said encrypted second message using a third public key to generate a second decrypted message; and

(c) comparing said second decrypted message to said second message.

16. The system of Claim 15 wherein said first public key, said second public key, said first message and said second message are stored in said set-top box.

17. The system of Claim 16 wherein said first digital certificate, said first private key and said first public key are issued by an independent certificate authority.

18. The system of Claim 17 wherein said first digital certificate is stored in said smart card.

19. The system of Claim 18 wherein said second digital certificate, said second private key and said second public key are issued by an independent certificate authority and are associated with said service provider.

20. The system of Claim 19 wherein said second digital certificate is stored in said service provider.